РАДИОТЕХНИКА И ЭЛЕКТРОНИКА, 2024, том 69, № 2, с. 137–145

ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ СИГНАЛОВ

УДК 621.396.621.59; 519.725

СИНХРОНИЗАЦИЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОЛДА НА ОСНОВЕ БЫСТРОГО ПРЕОБРАЗОВАНИЯ В УСЕЧЕННОМ БАЗИСЕ ФУНКЦИЙ УОЛША–АДАМАРА

© 2024 г. С. Ф. Горгадзе*, Д. Ву Ши, А. В. Ермакова

Московский технический университет связи и информатики (МТУСИ), ул. Авиамоторная, 8а, Москва, 111024 Российская Федерация

**E-mail: s.f.gorgadze@mtuci.ru*

Поступила в редакцию 19.10.2022 г.
После доработки 18.07.2023 г.
Принята к публикации 27.07.2023 г.

На основе анализа структур изоморфных мультипликативных групп расширенных полей Галуа установлено, что любой циклический сдвиг псевдослучайной последовательности Голда может быть преобразован к функции, принадлежащей к полному набору аналогов функций Радемахера соответствующей размерности. Это позволило разработать новый алгоритм быстрой синхронизации последовательностей Голда на основе вычисления их дискретной свертки с использованием быстрого спектрального преобразования в усеченном базисе функций Уолша–Адамара. Выигрыш разработанного алгоритма по числу арифметических операций по сравнению с традиционным способом вычисления дискретной свертки увеличивается с ростом длины последовательности N и при $N = 511.1023$ составляет приблизительно 3.4 раза.

Ключевые слова: изоморфные мультипликативные группы расширенных полей Галуа, псевдослучайная последовательность Голда, функции Радемахера, усеченный базис функций Уолша–Адамара

DOI: 10.31857/S0033849424020045, **EDN:** KMVICC

ВВЕДЕНИЕ

Проблема быстрой синхронизации шумоподобных сложных сигналов (СлС), формируемых на основе псевдослучайных последовательностей (ПСП) Голда [1–6], используемых в настоящее время во многих радиосистемах, включая спутниковые радионавигационные [1], не решена. В последних работах, посвященных данной проблеме [5, 6], рассматриваются ПСП Голда, формируемые при помощи двоичного подкласса последовательностей Гордона–Милса–Велча (ГМВ-последовательности) [7], которые не существуют при $N = 2^m - 1$ где $m = 5, 7, 11, 13, 17, \ldots$. Учитывая, что отсутствуют ПСП Голда для $m = 8, 12, 16$, можно сделать вывод, что метод синхронизации ПСП Голда, предложенный в этих работах, может быть применим к ПСП лишь четырех длин, используемым в практических приложениях в настоящее время – 511, 1023, 16283, 32567. Основной проблемой данного подхода, используемого также и в более ранних работах [7, 8], но лишь применительно к ГМВ-последовательностям, является увеличение боковых пиков периодических автокорреляционных функций (ПАКФ) [9] коротких ПСП, к которым преобразуется исходная более длинная ПСП, по отношению к неизменному по величине центральному пику ПАКФ.

В работах [7, 8], посвященных разработке методов поиска (синхронизации) дискретных сигналов на основе быстрых методов декодирования кодов, рассматриваются не отдельные ПСП Голда, а коды Голда, образованные на основе двух предпочтительных М-последовательностей (МП), когда слова кода представляют собой разные по структуре ПСП [2, 3]. Очевидно, что решенная задача не имеет прямого отношения к проблеме синхронизации СлС по времени, поскольку необходимо рассматривать блоковый код, образованный циклическими сдвигами одной и той же ПСП Голда. Но, очевидно, в этих работах не удалось установить взаимосвязь между структурой матрицы-циркулянта ПСП Голда и изоморфными мультипликативными группа-

ми полей Галуа [10, 11], на основе которых построены предпочтительные МП, образующие его. Это объясняется тем, что в работах [7, 8], а также [12], указывается лишь на одну структуру исходных матриц-циркулянтов МП, не позволяющую выявить такую взаимосвязь. Строки таких матриц начинаются с блоков двоичных символов, соответствующих десятичным номерам этих строк при их двоично-десятичном кодировании. Указывается лишь на очевидную возможность преобразования такого рода матриц-циркулянтов МП к матрице Уолша–Адамара при перестановке ее столбцов по возрастанию значений элементов мультипликативной группы поля Галуа, построенного на основе исходного неприводимого примитивного полинома. Но, как показано в [13], в одном и том же поле Галуа существуют по меньшей мере четыре разные по структуре мультипликативные группы и показано, как на основе любой такой группы построить матрицу-циркулянт МП, соответствующую ей. Таким образом, тип мультипликативной группы, соответствующий матрице-циркулянту МП, рассмотренной в [7, 8, 12], не выявлен. И лишь в [13] показано, что преобразование матрицы-циркулянта МП, описанной выше, H_1 (см. [13]), и только для первообразного элемента группы $\boldsymbol{\alpha}^0{}_{\boldsymbol{H}_1} = [1\ 0\ 0\ 0\ 0]^T$ ($[\cdot]^T$ – обозначение операции транспонирования матрицы). Также показано, что в случае перестановки отсчетов входного СлС начиная с любого другого первообразного элемента этой группы или использования любой другой мультипликативной группы того же поля, указанная матрица не приводится к матрице Уолша–Адамара, т.е. при такой перестановке никакой циклический МП не приводится ни к какой функции Уолша без нулевого символа при их нумерации от нуля. Кроме того, очевидно, что, суммируя матрицы-циркулянты предпочтительных МП структуры, описанной выше, невозможно получить матрицу-циркулянт ПСП Голда, а лишь разные по структуре ПСП этого типа.

В [13] впервые рассматриваются упорядоченные матрицы-циркулянты МП любой размерности N, в которых каждая последующая строка матрицы сдвинута циклически на один символ, по сравнению с предыдущей строкой. В этом случае перестановка столбцов матрицы-циркулянта производится по возрастанию значений элементов мультипликативной группы поля Галуа, соответствующей виду сопровождающей матрицы полинома $\mathbf{H}_2$ (см. [13]). При этом любой циклический сдвиг МП может быть приведен к любой функции Уолша без нулевого символа при их нумерации от нуля в зависимости от выбора первообразного элемента $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$ данной группы, который и определяет структуру матрицы-циркулянта и циклический сдвиг ее первой строки. Но при данном значении $\boldsymbol{\alpha}^0{}_{\mathbf{H}_2}$ соответствие между преобразуемым циклическим сдвигом МП и функцией Уолша без нулевого символа при их нумерации от нуля является взаимно однозначным. Таким образом, все возможные матрицы-циркулянты МП, каждая последующая строка которой сдвинута циклически относительно предыдущей строки на один символ, приводятся к одной и той же матрице функций Уолша без нулевых символов при их нумерации от нуля. Строки этой матрицы упорядочены по степеням элементов мультипликативной группы поля Галуа с первообразным элементом $\boldsymbol{\alpha}^0{}_{\mathbf{H}_1} = [1\ 0\ \ldots\ 0\ 0]^T$ при сопровождающей матрице исходного полинома вида $\mathbf{H}_1$ [см. [13]).

Цель данной работы[1] – исследование способа построения матриц-циркулянтов ПСП Голда и взаимосвязи их структуры с изоморфными мультипликативными группами полей Галуа, а также способов приведения матриц-циркулянтов этих

ПСП к функциям Уолша с целью разработки быстрого способа синхронизации ПСП Голда при обработке шумоподобных СлС.

1. ПОСТРОЕНИЕ МАТРИЦЫ-ЦИРКУЛЯНТА ПСП ГОЛДА

Матрицы-циркулянты последовательностей Голда получим путем суммирования по модулю 2 (*mod* 2) матриц $\mathfrak{I}_{m,2,ц}$ (см. [13]) двух так называемых предпочтительных МП [3, 4, 9]. Пусть на основе сопровождающей матрицы $\mathbf{H}_2$ первого предпочтительного полинома и первообразного элемента $\boldsymbol{\alpha}^0{}_{1\mathbf{H}_2}$ построена матрица-циркулянт МП ${}^{1}\mathfrak{I}_{m,2,ц}$, а на основе матрицы $\mathbf{H}_2$, но второго предпочтительного полинома и первообразного элемента $\boldsymbol{\alpha}^{0+z}{}_{2\mathbf{H}_2}$ – матрица ${}^{2}\mathfrak{I}_{m,2,ц}$. Тогда матрицы-циркулянты всего набора последовательностей Голда, соответствующих этим двум предпочтительным МП, кроме них самих, можно описать как:

$$\mathfrak{I}_{m,2,ц.g}(z) = {}^{1}\mathfrak{I}_{m,2,ц} \oplus {}^{2}\mathfrak{I}_{m,2,ц}, \quad z = 0,\ldots N-1, \tag{1}$$

[1] Данная статья является продолжением [13], поэтому в дальнейшем используются обозначения, введенные в ней.

где $\oplus$ – обозначение операции суммирования по модулю 2.

В качестве примера матрица-циркулянт кода Голда, построенного на основе полиномов $f_5(x) = x^5 + x^4 + x^2 + x + 1$ и $f_5(x) = x^5 + x^3 + 1$ при $\boldsymbol{\alpha}^0{}_{1\mathbf{H}_2} = \boldsymbol{\alpha}^0{}_{2\mathbf{H}_2} = [1\,0\,0\,0\,0]^T$ и $z = 0$ приведена в табл. 1. Как видно, она является упорядоченной, т.е. каждая ее последующая строка циклически сдвинута на один символ, по сравнению с предыдущей (см. [16]).

На рис. 1 представлена периодическая взаимно корреляционная функция (ПВКФ) [2] $\chi_{\text{ПВКФ}}(i)$ этой ПСП Голда и МП, сформированной на основе второго из двух указанных выше полиномов. Значения ПВКФ при отрицательных i получены при зеркальном отображении графика относительно оси ординат. Таким образом, матрица, приведенная в табл.1, соответствует последовательности Голда, поскольку получена трехуровневая ПВКФ.

Таблица 1. Матрица-циркулянт кода Голда, соответствующая предпочтительным полиномам $f_5(x) = x^5 + x^4 + x^2 + x + 1$ и $f_5(x) = x^5 + x^3 + 1$ при $\boldsymbol{\alpha}^0{}_{1\mathbf{H}_2} = \boldsymbol{\alpha}^0{}_{2\mathbf{H}_2} = [1\,0\,0\,0\,0]^T$ и $z = 0$

Суммы по *mod* 2 циклических сдвигов МП	***k***																															***i***
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
	$[\alpha^k{}_{1\mathrm{H}2} + \alpha_{2\mathrm{H}2}]_{10}$																															
	0	0	1	2	4	8	16	1	2	5	11	23	15	30	29	27	23	15	30	28	24	16	0	1	2	4	9	18	4	8	16	
$x_{1,0,k} \oplus x_{2,0,k}$	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	**0**
$x_{1,1,k} \oplus x_{2,1,k}$	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	**1**
$x_{1,2,k} \oplus x_{2,2,k}$	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	**2**
$x_{1,3,k} \oplus x_{2,3,k}$	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	**3**
$x_{1,4,k} \oplus x_{2,4,k}$	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	**4**
$x_{1,5,k} \oplus x_{2,5,k}$	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	**5**
$x_{1,6,k} \oplus x_{2,6,k}$	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	**6**
$x_{1,7,k} \oplus x_{2,7,k}$	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	**7**
$x_{1,8,k} \oplus x_{2,8,k}$	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	**8**
$x_{1,9,k} \oplus x_{2,9,k}$	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	**9**
$x_{1,10,k} \oplus x_{2,10,k}$	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	**10**
$x_{1,11,k} \oplus x_{2,11,k}$	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	**11**
$x_{1,12,k} \oplus x_{2,12,k}$	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	**12**
$x_{1,13,k} \oplus x_{2,13,k}$	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	**13**
$x_{1,14,k} \oplus x_{2,14,k}$	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	**14**
$x_{1,15,k} \oplus x_{2,15,k}$	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	**15**
$x_{1,16,k} \oplus x_{2,16,k}$	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	**16**
$x_{1,17,k} \oplus x_{2,17,k}$	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	**17**
$x_{1,18,k} \oplus x_{2,18,k}$	1	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	**18**
$x_{1,19,k} \oplus x_{2,19,k}$	1	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	**19**
$x_{1,20,k} \oplus x_{2,20,k}$	1	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	**20**
$x_{1,21,k} \oplus x_{2,21,k}$	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	**21**
$x_{1,22,k} \oplus x_{2,22,k}$	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	**22**
$x_{1,23,k} \oplus x_{2,23,k}$	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	**23**
$x_{1,24,k} \oplus x_{2,24,k}$	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	**24**
$x_{1,25,k} \oplus x_{2,25,k}$	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	**25**
$x_{1,26,k} \oplus x_{2,26,k}$	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	**26**
$x_{1,27,k} \oplus x_{2,27,k}$	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	**27**
$x_{1,28,k} \oplus x_{2,28,k}$	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	**28**
$x_{1,29,k} \oplus x_{2,29,k}$	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	**29**
$x_{1,30,k} \oplus x_{2,30,k}$	1	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	**30**
$x_{1,31,k} \oplus x_{2,31,k}$	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	**0**
$x_{1,32,k} \oplus x_{2,32,k}$	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0	**1**

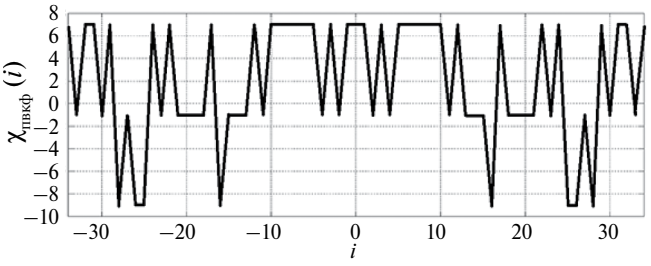

Рис. 1. Периодическая взаимно корреляционная функция кодов Голда.

Упорядоченная матрица-циркулянт кода Голда при выбранных значениях $\boldsymbol{\alpha}^0{}_{1\mathbf{H}_2}$, $\boldsymbol{\alpha}^0{}_{2\mathbf{H}_2}$ и z имеет следующий вид:

$$\mathfrak{I}_{m,2,u.g}(z)=\begin{bmatrix}\mathfrak{I}_{m,2}{}^1\oplus\mathfrak{I}_{m,2}{}^2\\ \mathbf{H}_{21}{}^m\mathfrak{I}_{m,2}{}^1\oplus\mathbf{H}_{22}{}^m\mathfrak{I}_{m,2}{}^2\\ \mathbf{H}_{21}{}^{2m}\mathfrak{I}_{m,2}{}^1\oplus\mathbf{H}_{22}{}^{2m}\mathfrak{I}_{m,2}{}^2\\ \dots\\ \mathbf{H}_{21}{}^{C(N)m}\mathfrak{I}_{m,2}{}^1\oplus\mathbf{H}_{22}{}^{C(N)m}\mathfrak{I}_{m,2}{}^2\end{bmatrix}, \quad (2)$$

где $\mathfrak{I}_{m,2}{}^1$ – матрица из m циклических сдвигов первой предпочтительной МП, построенная на основе сопровождающей матрицы $\mathbf{H}_{21}$ ее неприводимого примитивного полинома, $\mathfrak{I}_{m,2}{}^2$ – соответствующая матрица для второй предпочтительной МП, построенная на основе сопровождающей матрицы $\mathbf{H}_{22}$ ее неприводимого примитивного полинома. В индексах обозначений сопровождающих матриц $\mathbf{H}_{21}$ и $\mathbf{H}_{22}$ первый символ 2 указывает на то, что рассматриваются матрицы вида $\mathbf{H}_2$, а второй символ 1 или 2 – на отношение матрицы к первому или второму предпочтительному полиному.

Очевидно, что столбцы первых m строк матрицы (2) представляют собой суммы степеней первообразных элементов двух мультипликативных групп, т.е.

$$\mathfrak{I}_{m,2}{}^1\oplus\mathfrak{I}_{m,2}{}^2=\boldsymbol{\alpha}^k{}_{1\mathbf{H}_2}+\boldsymbol{\alpha}^k{}_{2\mathbf{H}_2},\ k=0,\dots,N-1, \quad (3)$$

и значения $[\boldsymbol{\alpha}^k{}_{1\mathbf{H}_2}+\boldsymbol{\alpha}^k{}_{2\mathbf{H}_2}]_{10}$ могут совпадать для разных k. Кроме того, в (2) возможно появление элементов, состоящих лишь из нулей, т.е. сумма изоморфных максимальных мультипликативных групп двух разных полей Галуа не образует мультипликативную группу.

2. ПРЕОБРАЗОВАНИЕ МАТРИЦЫ-ЦИРКУЛЯНТА ПСП ГОЛДА К АНАЛОГАМ ФУНКЦИЙ РАДЕМАХЕРА

Преобразовав символы $\boldsymbol{\alpha}^k{}_{1\mathbf{H}_2}+\boldsymbol{\alpha}^k{}_{2\mathbf{H}_2}$ по правилу $0\to 1, 1\to -1$ и переставив столбцы (2) по возрастанию $\left[\boldsymbol{\alpha}^k{}_{1\mathbf{H}_2}+\boldsymbol{\alpha}^k{}_{2\mathbf{H}_2}\right]_{10}$, одновременно суммируя одинаковые их значения и заменяя отсутствующие элементы нулями, получим функции, у которых имеются символы, отличные от 1 или −1, а также символы с нулевыми значениями. Так, переставляя в соответствии с данным правилом столбцы матрицы, приведенной в табл. 1, получим матрицу, записанную в строках табл. 2.

Как видно, половина символов преобразованной матрицы, записанных в ее второй строке, положительные или нули, половина отрицательные или нули, в третьей строке первые восемь символов положительные или нули, потом следуют восемь отрицательных или нулевых символов, потом опять восемь положительных, потом восемь отрицательных и т.д. То есть первые m строк матрицы-циркулянта последовательности Голда, преобразованные по описанному правилу, являются аналогами функций Радемахера [13] (обозначим их как r_{ia}, где $i = 0, \dots, (m-1)$ – номер функции), но остальные строки исходной матрицы-циркулянта не приводятся к аналогам функций Уолша без нулевого символа при их нумерации с нуля. Обозначим их как r'_i, где $i=m,\dots,((C(N)+1)m-1)$, $C(N)=\left(\frac{A(N)}{m}\right)-1$, $A(N)-$ число, максимально близкое к N, делящееся нацело на m и удовлетворяющее неравенству $A(N) > N$ [16]. Но функции r'_i могут быть приведены к аналогам функций Радемахера при выборе соответствующих первообразных элементов мультипликативных групп. То есть выбрав $\boldsymbol{\alpha}^0{}_{1\mathbf{H}_2}$ и $\boldsymbol{\alpha}^0{}_{2\mathbf{H}_2}$ и переставив столбцы матрицы-циркулянта кода Голда по возрастанию $\left[\boldsymbol{\alpha}^k{}_{1\mathbf{H}_2}+\boldsymbol{\alpha}^k{}_{2\mathbf{H}_2}\right]_{10}$, преобразуем первые ее m строк к матрице аналогов функций Радемахера. Но если столбцы этой матрицы переставлять начиная с элемента $\boldsymbol{\alpha}^m{}_{1\mathbf{H}_2}+\boldsymbol{\alpha}^m{}_{2\mathbf{H}}$, то к аналогам функций Радемахера преобразуются вторые m строк матрицы-циркулянта кода Голда. При перестановке начиная с $\boldsymbol{\alpha}^{2m}{}_{1\mathbf{H}_2}+\boldsymbol{\alpha}^{2m}{}_{2\mathbf{H}_2}$ преобразуем следующие m строк и т.д. Данный подход к приведению циклических сдвигов кода Голда к аналогам функций Радемахера имеет смысл только в том случае, если существует ускоренный алгоритм умножения матрицы функций Радемахера на вектор, вычислительная сложность которого соответствует числу элементарных математических операций, значимо меньшему mN,

Таблица 2. Результат преобразования матрицы-циркулянта кода Голда по возрастанию значений суммы мультипликативных групп

Преобразованные циклические сдвиги ПСП Голда	k																														i
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
$\boldsymbol{r}_{0a}$	3	3	3	0	3	1	0	0	2	1	0	1	0	0	0	2	–3	0	–1	0	0	0	0	–2	–1	0	0	–1	–1	–1	–2	**0**
$\boldsymbol{r}_{1a}$	3	3	3	0	3	1	0	0	–2	–1	0	–1	0	0	0	–2	3	0	1	0	0	0	0	2	–1	0	0	–1	–1	–1	–2	**1**
$\boldsymbol{r}_{2a}$	3	3	3	0	–3	–1	0	0	2	1	0	1	0	0	0	–2	3	0	1	0	0	0	0	–2	1	0	0	1	–1	–1	–2	**2**
$\boldsymbol{r}_{3a}$	3	3	–3	0	3	1	0	0	2	1	0	–1	0	0	0	–2	3	0	–1	0	0	0	0	–2	1	0	0	–1	1	1	–2	**3**
$\boldsymbol{r}_{4a}$	3	–3	3	0	3	–1	0	0	2	–1	0	–1	0	0	0	–2	3	0	1	0	0	0	0	–2	1	0	0	–1	1	–1	2	**4**
$\boldsymbol{r}'_{5}$	–1	3	1	0	1	–1	0	0	2	1	0	–1	0	0	0	2	1	0	1	0	0	0	0	–2	1	0	0	–1	1	–1	0	**5**
$\boldsymbol{r}'_{6}$	1	1	–1	0	3	–1	0	0	0	1	0	–1	0	0	0	0	1	0	1	0	0	0	0	2	1	0	0	–1	1	–1	0	**6**
$\boldsymbol{r}'_{7}$	3	–1	1	0	1	–1	0	0	2	1	0	1	0	0	0	0	–1	0	1	0	0	0	0	0	–1	0	0	1	1	–1	0	**7**
$\boldsymbol{r}'_{8}$	1	1	–1	0	3	1	0	0	–2	1	0	–1	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	1	–1	1	0	**8**
$\boldsymbol{r}'_{9}$	3	–1	3	0	–1	–1	0	0	0	1	0	–1	0	0	0	0	–1	0	1	0	0	0	0	0	1	0	0	1	1	1	0	**9**
$\boldsymbol{r}'_{10}$	1	3	–1	0	1	–1	0	0	0	1	0	–1	0	0	0	0	1	0	–1	0	0	0	0	0	–1	0	0	1	1	1	2	**10**
$\boldsymbol{r}'_{11}$	1	–1	–1	0	1	–1	0	0	0	–1	0	–1	0	0	0	2	3	0	1	0	0	0	0	0	1	0	0	1	–1	1	2	**11**
$\boldsymbol{r}'_{12}$	1	–1	–1	0	–1	–1	0	0	2	1	0	1	0	0	0	2	–1	0	1	0	0	0	0	2	1	0	0	–1	1	1	0	**12**
$\boldsymbol{r}'_{13}$	–1	–1	–3	0	3	1	0	0	–2	1	0	1	0	0	0	0	1	0	1	0	0	0	0	2	1	0	0	1	1	–1	2	**13**
$\boldsymbol{r}'_{14}$	–1	–3	3	0	–1	1	0	0	0	1	0	1	0	0	0	2	–1	0	1	0	0	0	0	0	1	0	0	1	1	1	0	**14**
$\boldsymbol{r}'_{15}$	–3	3	1	0	1	1	0	0	–2	1	0	1	0	0	0	0	–1	0	–1	0	0	0	0	2	1	0	0	–1	1	1	2	**15**
$\boldsymbol{r}'_{16}$	1	1	1	0	–1	1	0	0	–2	–1	0	1	0	0	0	2	–1	0	1	0	0	0	0	0	1	0	0	1	1	–1	2	**16**
$\boldsymbol{r}'_{17}$	1	1	1	0	–3	1	0	0	0	1	0	–1	0	0	0	2	1	0	–1	0	0	0	0	2	–1	0	0	1	1	1	0	**17**
$\boldsymbol{r}'_{18}$	–1	1	–1	0	1	–1	0	0	0	–1	0	1	0	0	0	0	3	0	–1	0	0	0	0	2	1	0	0	1	–1	1	2	**18**
$\boldsymbol{r}'_{19}$	–1	–1	1	0	–1	1	0	0	2	–1	0	1	0	0	0	2	1	0	–1	0	0	0	0	0	1	0	0	1	1	1	0	**19**
$\boldsymbol{r}'_{20}$	–3	1	1	0	1	1	0	0	0	–1	0	–1	0	0	0	0	1	0	–1	0	0	0	0	2	1	0	0	1	1	1	2	**20**
$\boldsymbol{r}'_{21}$	1	1	1	0	–1	–1	0	0	0	–1	0	1	0	0	0	2	–3	0	1	0	0	0	0	0	1	0	0	1	1	1	2	**21**
$\boldsymbol{r}'_{22}$	1	1	–1	0	–1	1	0	0	–2	1	0	1	0	0	0	2	1	0	–1	0	0	0	0	2	–1	0	0	–1	1	1	2	**22**
$\boldsymbol{r}'_{23}$	1	–1	1	0	–1	1	0	0	0	–1	0	1	0	0	0	2	1	0	–1	0	0	0	0	2	1	0	0	1	–1	–1	2	**23**
$\boldsymbol{r}'_{24}$	1	1	1	0	–1	1	0	0	2	–1	0	1	0	0	0	2	–1	0	–1	0	0	0	0	2	–1	0	0	1	1	1	–2	**24**
$\boldsymbol{r}'_{25}$	1	1	1	0	1	1	0	0	0	–1	0	1	0	0	0	–2	1	0	–1	0	0	0	0	2	–1	0	0	1	–1	1	2	**25**
$\boldsymbol{r}'_{26}$	1	1	1	0	–1	1	0	0	2	–1	0	1	0	0	0	2	1	0	1	0	0	0	0	–2	–1	0	0	1	–1	1	0	**26**
$\boldsymbol{r}'_{27}$	–1	1	–1	0	1	1	0	0	2	1	0	–1	0	0	0	0	3	0	1	0	0	0	0	2	–1	0	0	–1	–1	1	0	**27**
$\boldsymbol{r}'_{28}$	1	–1	1	0	3	–1	0	0	2	1	0	1	0	0	0	0	–1	0	1	0	0	0	0	0	1	0	0	1	–1	–1	0	**28**
$\boldsymbol{r}'_{29}$	–1	1	1	0	3	1	0	0	0	1	0	1	0	0	0	0	1	0	1	0	0	0	0	0	–1	0	0	–1	1	1	–2	**29**
$\boldsymbol{r}'_{30}$	–1	1	3	0	1	1	0	0	2	1	0	1	0	0	0	–2	1	0	1	0	0	0	0	0	–1	0	0	–1	–1	–1	2	**30**
$\boldsymbol{r}_{0a}$	3	3	3	0	3	1	0	0	2	1	0	1	0	0	0	2	–3	0	–1	0	0	0	0	–2	–1	0	0	–1	–1	–1	–2	**0**
$\boldsymbol{r}_{1a}$	3	3	3	0	3	1	0	0	–2	–1	0	–1	0	0	0	–2	3	0	1	0	0	0	0	2	–1	0	0	–1	–1	–1	–2	**1**
$\boldsymbol{r}_{2a}$	3	3	3	0	–3	–1	0	0	2	1	0	1	0	0	0	–2	3	0	1	0	0	0	0	–2	1	0	0	1	–1	–1	–2	**2**

поскольку именно такая сложность соответствует умножению матрицы размером $m \times N$ на столбец.

3. БЫСТРЫЙ АЛГОРИТМ СИНХРОНИЗАЦИИ ПСП ГОЛДА

Функции Радемахера располагаются в строках матрицы Адамара $\mathbf{A}_m$ порядка 2^m с номерами $y = 2^v, v = 0, 1, 2, 3 \ldots 2^{m-1}$ (например, при $m = 5$ – в строках с номерами 1, 2, 4, 8, 16, при $m = 9$ – в строках с номерами 1, 2, 4, 8, 16, 32, 64, 128, 256, при $m = 10$ – в строках с номерами 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 и т.д.). Матрица $\mathbf{A}_m$ может быть представлена в виде простого произведения слабо заполненных матриц $\mathbf{B}_1$, $\mathbf{B}_2$,..., $\mathbf{B}_m$.

В наиболее простом варианте такого представления $\mathbf{B}_1 = \mathbf{B}_2 = \ldots == \mathbf{B}_m = \mathbf{B}$, где

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & 1 & \ldots & 0 & 0 \\ & & & \ldots & & & \\ 0 & 0 & 0 & 0 & \ldots & 1 & 1 \\ 1 & -1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & -1 & \ldots & 0 & 0 \\ & & & \ldots & & & \\ 0 & 0 & 0 & 0 & \ldots & 1 & -1 \end{bmatrix}, \quad (4)$$

т.е. $\mathbf{A}_m = \mathbf{B}_1\mathbf{B}_2\ldots\mathbf{B}_m = \mathbf{B}^m$. Размерность матрицы $\mathbf{A}_m$ равняется 2^m, а нумерация ее строк начинается с нуля [14].

Сохраняя в матрице $\mathbf{A}_m$ только m строк с номерами y из общего их числа, равного 2^m, получим усеченную матрицу Адамара, алгоритм факторизации которой описан в [15, 16]. Так, в матрице $\mathbf{B}_1$ сохраняются только m строк с теми же номерами $y = 2^v, v = 0,1,2,3\ldots 2^{m-1}$, которые были сохранены в матрице $\mathbf{A}_m$, т.е. при умножении полученной усеченной матрицы $\mathbf{B}_{1y}$ на результат умножения $\mathbf{B}_{2y}\ldots\mathbf{B}_{my}$ на входной вектор $\mathbf{X}$ потребуется лишь m операций суммирования. Матрицу $\mathbf{B}_{2y}$ получим, учитывая, что $(N - 2m)$ столбцов матрицы $\mathbf{B}_{1y}$ состоят только из нулевых элементов. Эти столбцы тоже надо исключить из $\mathbf{B}_{1y}$, одновременно исключая строки матрицы $\mathbf{B}_2$, номера которых совпадают с номерами столбцов, исключенных в $\mathbf{B}_{1y}$, поэтому матрица $\mathbf{B}_{2y}$ содержит $2m$ строк, и при умножении ее на $\mathbf{B}_3\ldots\mathbf{B}_m\mathbf{X}$ потребуется лишь $2m$ операций суммирования, в последней матрице $\mathbf{B}_{my}$ всегда сохраняется 2^m строк, т.е $\mathbf{B}_{my} = \mathbf{B}$.

Таким образом, число строк, сохраняемых в матрицах $\mathbf{B}_{sy}$, $s = 1,\ldots,m$ и совпадающее с числом элементарных операций суммирования, которое надо произвести для перемножения вектора с каждой матрицей, описывается как $m + 2m + (2 \cdot 2m - 4) + (2 \cdot (2 \cdot 2m - 4) - 8) + + (2 \cdot (2 \cdot (2 \cdot 2m - 4) - 8) - 16) + \ldots$

Можно вывести рекуррентную формулу для расчета числа ненулевых строк матриц $\mathbf{B}_{sy}$:

$$B(s) = \begin{cases} m, \text{ если } s = 1, \\ 2m, \text{ если } s = 2, \\ 2B(s-1) - 2^{s-1}, \text{ если } s = 3,4,\ldots, \end{cases} \quad (5)$$

где $B(s)$ – число строк, сохраняемых в матрице $\mathbf{B}_{sy}$. Тогда число арифметических операций суммирования при ускоренном умножении матрицы из функций Радемахера на вектор:

$$S = B(1) + B(2) + \sum_{s=3}^{m} 2B(s-1) - 2^{s-1}, \quad (6)$$

а выигрыш в числе таких операций, по сравнению с простым перемножением матрицы такой же размерности на вектор, составит $I(m) = m2^m / S$. Оценить значимость этого выигрыша можно, анализируя рис. 2.

Как видно, при $m = 5$ он составляет примерно 1.84, но при типичных длинах ПСП, использующихся при построении, например, навигационных кодов, он более существенный – при $N = 511(m = 9)$ выигрыш составляет 3 раза, а при $N = 1023$ $(m = 10)$ – 3.4 раза. Подчеркнем, что на рис. 2 приводится выигрыш в числе арифметических операций при ускоренном перемножении матрицы функций Радемахера и вектора, по сравнению с простым перемножением. Для того чтобы не разрывать график, показаны значения выигрыша при m = 8, 12 и 16, хотя ПСП Голда при таких значениях m не существует [8].

Таким образом, предлагаемый алгоритм синхронизации последовательностей Голда на основе быстрого преобразования Адамара (БПА) при заданном циклическом сдвиге предпочтительных МП z состоит в следующем:

1) с целью обеспечения возможности синхронизации всего набора последовательностей Голда, для формирования которых используется данная пара предпочтительных МП, выбрать $\boldsymbol{\alpha}^0{}_{1\mathbf{H}_2}$ и $\boldsymbol{\alpha}^0{}_{2\mathbf{H}_2}$ мультипликативных групп их полей Галуа и найти суммы $\boldsymbol{\alpha}^k{}_{1\mathbf{H}_2} + \boldsymbol{\alpha}^{k(z)}{}_{2\mathbf{H}_2}$, где

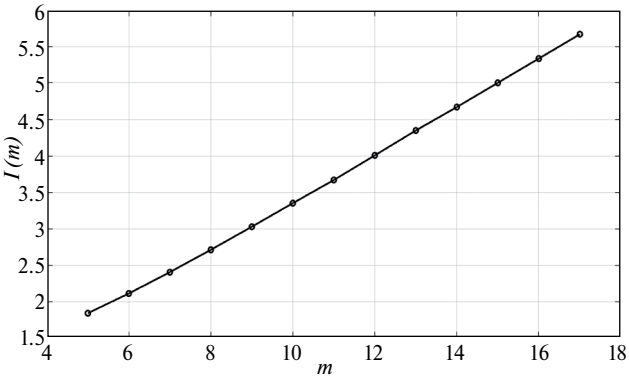

Рис. 2. Выигрыш в числе элементарных математических операций при ускоренном перемножении матрицы функций Радемахера и вектора по сравнению с простым перемножением.

$k(z) = k + z$ при $k + z \le N$ и $k(z) = k + z - N$ при $k + z > N, k = 0,\ldots,N-1$;

2) переставить значения входного дискретного сигнала $\mathbf{X}_N$, содержащего последовательность Голда с неизвестным циклическим сдвигом, по возрастанию значений $\left[\boldsymbol{\alpha}^{k}{}_{1\mathbf{H}_2} + \boldsymbol{\alpha}^{k(z)}{}_{2\mathbf{H}_2}\right]_{10}$, записывая эти символы в ячейки памяти с соответствующими номерами; если адреса записи разных символов совпадают, то они записываются в одну и ту же ячейку и суммируются; элементы $\left[\boldsymbol{\alpha}^{k}{}_{1\mathbf{H}_2} + \boldsymbol{\alpha}^{k(z)}{}_{2\mathbf{H}_2}\right]_{10}$, состоящие лишь из нулей, определяют запись символа входного кода в нулевую ячейку и суммирование с ранее записанными в нее символами; содержимое ячеек, оставшихся пустыми, обнуляется;

3) полученный вектор, значения символов которого записаны в запоминающее устройство, ускоренно перемножается с матрицей функций Радемахера; полученные m значений результата перемножения соответствуют m значениям ПАКФ последовательности Голда;

4) для идентификации основного пика ПАКФ в данном случае целесообразно использовать пороговый алгоритм; если этот пик оказался среди полученных значений ПАКФ – процедура синхронизации завершается; если нет – выполняется следующий пункт;

5) значения $\boldsymbol{X}_N$ вновь переставляются по правилу, описанному выше, но уже по возрастанию значений $\left[\boldsymbol{\alpha}^{k+m}{}_{1\mathbf{H}_2} + \boldsymbol{\alpha}^{k(z)+m}{}_{2\mathbf{H}_2}\right]_{10}$; после перемножения полученного вектора с матрицей функций Радемахера, получаем следующие m значений ПАКФ последовательности Голда и т.д.;

6) для синхронизации другой последовательности Голда надо изменить значение $z = 0,\ldots N-1$.

В соответствии с описанным алгоритмом была вычислена ПАКФ ПСП Голда, матрица-циркулянт которого приведена в табл. 1. Соответствующий график приведен на рис. 3, а на рис. 4 показана ПАКФ этой ПСП Голда, полученная при простом перемножении ее матрицы-цир-

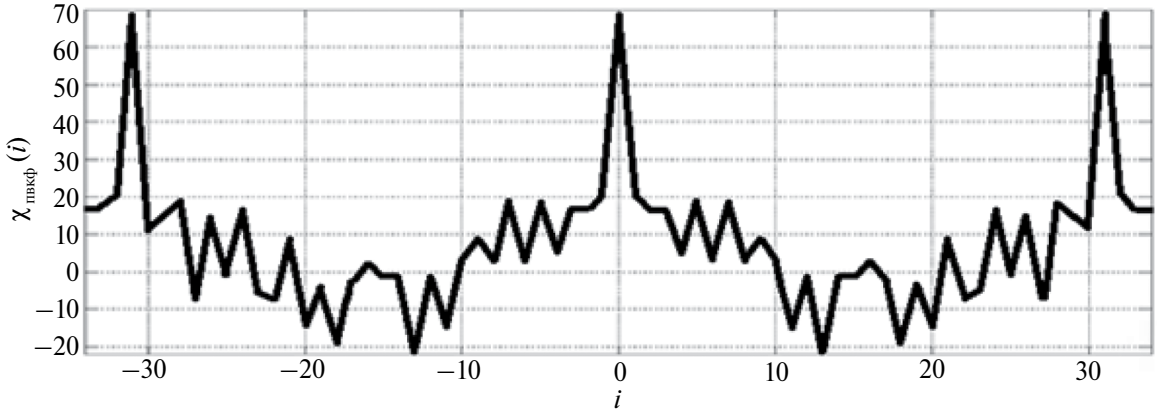

Рис. 3. Результат ускоренного вычисления ПАКФ кода Голда ($m = 5$).

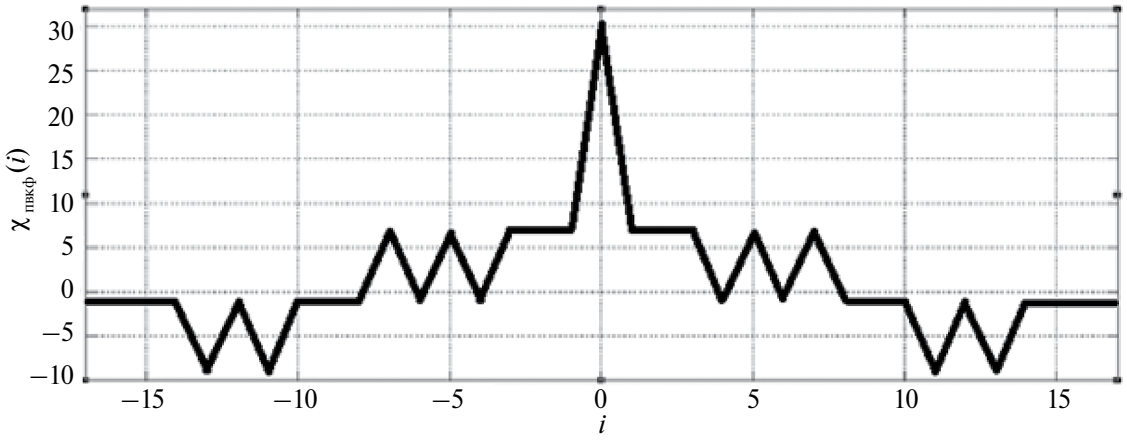

Рис. 4. Периодическая взаимно корреляционная функция кода Голда ($m = 5$).

кулянта с ее первой строкой, транспонированной в столбец. Незначительное отличие ПАКФ одной и той же последовательности, вычисленных разными способами, объясняется разными значениями длины ПСП Голда и функции Радемахера–Уолша. Появление дополнительных основных пиков на рис. 2 по бокам основного пика объясняется отличием размерности матрицы-циркулянта ПСП Голда и матрицы Адамара.

Таким образом, при традиционном способе вычисления ПАКФ необходимо последовательно сдвигать опорную ПСП относительно значений принимаемого дискретного сигнала на один символ с последующим вычислением одного значения ПАКФ, для чего потребуется N операций перемножения с накоплением. В результате вычисление всей ПАКФ потребует N сдвигов опорной ПСП относительно принимаемого сигнала и N^2 операций перемножения с накоплением. В предлагаемом алгоритме число перестановок символов последовательности равно $\frac{A(N)}{m}$, и после каждой из них вычисляется сразу m значений ПАКФ с существенно меньшим числом элементарных операций суммирования, чем при вычислении m значений ПАКФ традиционным способом. Выигрыш в числе арифметических операций предлагаемого алгоритма, по сравнению с традиционным, в зависимости от значения m соответствует графику, приведенному на рис. 2. Отметим, что правило перестановки символов входного дискретного сигнала задается тем же генератором последовательности Голда, который используется и при формировании опорного сигнала в традиционном алгоритме вычисления ПАКФ.

ЗАКЛЮЧЕНИЕ

Первые m строк любой упорядоченной матрицы-циркулянта последовательности Голда могут быть приведены к аналогам функций Радемахера путем перестановки ее столбцов по возрастанию значений суммы максимальных мультипликативных групп двух предпочтительных неприводимых примитивных полиномов, на основании которых построен данный код. При этом структура групп определяется сопровождающими матрицами предпочтительных полиномов вида $\boldsymbol{H}_2$. При сдвиге первообразных элементов суммируемых мультипликативных групп на m элементов следующие m строк исходной матрицы приводятся к функциям Радемахера, при сдвиге на $2m$ элементов – следующие и т.д.

Преобразование последовательности Голда в соответствии с п. 1 Заключения позволяет быстро вычислить его ПАКФ с помощью БПА в усеченном базисе функций Уолша–Адамара, причем выигрыш по числу элементарных операций в зависимости от длины ПСП $N = 2^m - 1$, по сравнению с корреляционным алгоритмом, соответствует рис. 2.

Авторы заявляют об отсутствии конфликта интересов.

СПИСОК ЛИТЕРАТУРЫ

1. *Maral G., Bousquet M., Sun Z.* Satellite Communications Systems. United Kingdom: Wiley, 2020.
2. *Gold R.* // IEEE Trans. 1967. V. IT-13. № 4. P. 619. https://doi.org/10.1109/TIT.1967.1054048
3. *Кузнецов В.С., Шевченко И.В., Волков А.С., Солодков А.В.* // Труды МАИ. 2017. Вып. 96. https://trudymai.ru/upload/iblock/f64/Kuznetsov_Hevchenko_Volkov_Solodkov_rus.ru&issue=96
4. *Кузнецов В.С., Мордасов К.А.* // Изв. вузов. Электроника. 2010. № 1. С. 57.
5. *Михайлов В.Ю., Мазепа Р.Б.* // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 4. С. 4.
6. *Michaylov V. Yu., Mazepa R.B.* // Systems of Signal Generating and Processing in the Field of on Board Communications: Conf. Proc. 2021. P. 9416089.
7. *Лосев В.В., Бродская Е.Б., Коржик В.И.* Поиск и декодирование сложных дискретных сигналов. М.: Радио и связь, 1988.
8. *Лосев В.В., Дворников В.Д.* // РЭ. 1983. Т. 28. № 8. С. 1540.
9. *Варакин Л.Е.* Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985.
10. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976.
11. *Свердлик М.Б.* Оптимальные дискретные сигналы. М.: Сов. радио, 1975.
12. *Канатова Л.В., Литвинов В.Л., Финк Л.М.* // Проблемы передачи информации. 1986. Т. 22. Вып. 2. С. 98.
13. *Горгадзе С.Ф., Ву Ши Д., Ермакова А.В.* // РЭ. 2024. Т. 69. № 2. С.
14. *Трахтман А.М., Трахтман В.А.* Основы теории дискретных сигналов на конечных интервалах. М.: Сов. радио, 1975.
15. *Горгадзе С.Ф.* // РЭ. 2005. Т. 50. № 3. С. 302.
16. *Горгадзе С.Ф.* // РЭ. 2006. Т. 51. № 4. С. 428.

SYNCHRONIZATION OF GOLD SEQUENCES BASED ON FAST TRANSFORM IN A TRUNCATED BASIS OF WALSH–HADAMARD FUNCTIONS

S. F. Gorgadze*, Dao Vu Shi, A. V. Ermakova

Moscow Technical University of Communication and Information, Moscow 111024 Russia

**E-mail: s.f.gorgadze@mtuci.ru*

Received October 19, 2022; revised July 18, 2023; accepted July 27, 2023

Based on the analysis of the structures of isomorphic multiplicative groups of extended Galois fields, it is established that any cyclic shift of a pseudo-random Gold sequence can be transformed into a function belonging to the complete set of analogues of Rademacher functions of the corresponding dimension. This made it possible to develop a new algorithm for fast synchronization of Gold sequences based on the calculation of their discrete convolution using fast spectral transformation in a truncated basis of Walsh–Hadamard functions. The gain of the developed algorithm in terms of the number of arithmetic operations compared to the traditional method of calculating discrete convolution increases with increasing sequence length N and for N=511.1023 is approximately 3.4 times.

Keywords: isomorphic multiplicative groups of extended Galois fields, pseudo-random Gold sequence, Rademacher functions, truncated basis of Walsh–Hadamard functions